"EXPRESS MAIL" MAILING LABEL NUMBER EL 701970038US
DATE OF DEPOSIT JULY 11, 2001
I HEREBY CERTIFY THAT THIS PAPER OR FEE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE "EXPRESS MAIL POST OFFICE TO ADDRESSEE" SERVICE UNDER 37 C.F.R. 1.10 ON THE DATE INDICATED ABOVE AND IS ADDRESSED TO ASSISTANT COMMISSIONER FOR TRADEMARKS 2900 CRYSTAL DRIVE, ARLINGTON, VA 22202-3513

Kimberly A. Lawrence
(TYPED OR PRINTED NAME OF PERSON MAILING PAPER OR FEE)

SIGNATURE 7-11-01 Date

FIELD OF THE INVENTION

[0001] The present invention relates to a method and apparatus for providing trusted access to a network, and more particularly, to a method and apparatus for providing access to authenticated documents over a network.

BACKGROUND

[0002] Advances in technology provide increasing capabilities for electronic file duplication and transport making the sharing over a network of electronic documents increasingly easy. The ability to provide nearly instant access to information to millions of users has revolutionized the way many businesses are run. However, it is well known to those who practice in the art that electronic files are easily corrupted, that even secure systems connected to network can be attacked and breached with the subsequent corruption of files. As such, in the current environment, users who receive files from many network sources are unable to verify the authenticity of the files received.

[0003] Many applications in a wide range of fields require the ability to provide trusted access to networks. For example, schools or other institutions may need to provide students access to the Internet without fear of exposing the students to inappropriate material. In the financial and insurance industries many documents are forwarded electronically without any guarantee as to the authenticity of the contents thereof.

[0004] Known in the art are filtering techniques which attempt to programmatically identify objectionable or non-authentic material both in print and picture formats. Some create lists to objectionable sites to which access is denied. These methods are often prone to error and circumvention as the lists which allow or

block access are constantly required to be updated and are vulnerable to low level network traffic which could allow objectionable or other unauthorized material into the system being filtered. Therefore, there is a need for an apparatus and method for providing trusted access to networks wherein the contents of electronic documents received over a network can be authenticated.

SUMMARY OF THE INVENTION

[0005] Accordingly, an apparatus and method for providing access to authenticated electronic documents over a network is disclosed. The apparatus includes a server computer having a user interface connected thereto via a first network interface for providing user access to the server. A second network interface connects the server to a computer network containing the electronic documents. A third network interface connects a database to the server. The database stores data for authenticating the electronic documents. The first network interface, second network interface and third network interface are disjunct respective to each other such that the user, the computer network and the database are not in communication therebetween. A verification server having first and second network interfaces connect the computer network and the database to the verification server respectively. The first and second network interfaces connected to the verification server are disjunct, such that the database is not accessible to the computer network. The apparatus according to the present invention provides a user access to authenticated electronic documents contained on a computer network.

[0006] Additionally, a method of providing access to authenticated electronic documents over a network is disclosed. The method includes the steps of: 1) Initializing a database by storing indexed information for identifying and authenticating the electronic documents therein; 2) Receiving a user request for an electronic document; 3) Searching for and retrieving information for identifying and authenticating the requested document from the database; 4) Accessing the network and retrieving the content of the requested document; 5) Calculating a checksum or sum value for the content of the retrieved document; 6) Comparing the sum value calculated for the retrieved document with the authenticating information retrieved from the database for the particular document; 7) Determining if the document is authentic; 8) Returning the contents of the document to the user if the contents are determined authentic; 9) Returning a refusal to the to the user if the content of the

retrieved document is not authentic or if the requested document is not indexed in the database; and 10) Updating the database accordingly with the status of the authenticity of the electronic document. The method according to the present invention allows a user to access authenticated electronic documents contained on a computer network.

[0007] One advantage associated with the present invention is the ability to provide trusted access to a computer network.

[0008] Another advantage associated with the invention is the ability to provide access to selected and authenticated electronic documents contained within a computer network.

[0009] Another advantage associated with the invention is the ability to identify the content of electronic documents as trusted or not trusted which is based on a review by individuals. Each document for which access is provided is reviewed individually as to the subject matter or accuracy of the content thereof and after approval, the document is indexed accordingly in the database including randomly generated seed values which are used thereafter to verify the authenticity of the document. Additionally, denial to objectionable material or other not authorized material is automatic as the network is not accessible to the user directly.

[0010] Another advantage associated with the present invention is the use of disjunct interfaces to connect the user interface, the network, and the database to the server computer and the verification server to eliminate unauthorized access to the network or the database.

[0011] Another advantage is the use of the verification server to iteratively traverse the database containing indexed information for the electronic documents for which access is provided and to retrieve the content of each document, check the authenticity thereof and update the database according with the authenticity status of the particular document, thereby providing for access to authentic electronic documents.

[0012] Another advantage is the use of a two pass method of calculating checksums for authenticating the content of electronic documents.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] FIGS. 1 –3 are block diagrams of various embodiments of the apparatus of the present invention;

FIG. 4 is a flow chart representing the method for providing access to authenticated documents over a network according to the present invention;

FIG. 5 is a is a flow chart representing one embodiment of the method of calculating checksums for authenticating the content of electronic documents according to the present invention;

FIG. 6 is a flow chart representing one embodiment of the verification server of the present invention; and

FIG. 7 is a diagram of one embodiment of the format of a database according to the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0014] A detailed description of the preferred embodiments of the invention follows. It is to be understood that the disclosed embodiments are merely exemplary of the invention, which may be embodied in various forms. Therefore, specific structural and functional details disclosed are not to be interpreted as limiting, but rather as a representative basis for teaching one skilled in the art to variously employ the present invention in virtually any appropriately detailed system or structure. It should be understood that the drawings included herewith represent preferred embodiments of the invention only and are included to facilitate an understanding of the invention and not to limit the scope thereof.

[0015] Referring to the drawings, wherein like numerals represent like elements throughout the several views, Figure 1 is a diagram of an apparatus constructed according to one embodiment of the present invention, generally 100, including user 10 having access to computer 12. Computer 12 is connectable to server 16 via public network 14. Server computer 16 comprises a first network interface 18 connected to public network 14 for providing user access to server 16 and connecting server 16 to public network 14. A second network interface 20 connects server 16 to private network 15 for retrieving data from networks 15. A third network interface 22 connects server 16 to database 24. Network interfaces 18, 20, and 22 are disjunct with respect to each other, such that user 10, networks 14 and 15, and database 24 are not in direct communication therebetween. Server 16 can be

configured using individual network cards for each of the interfaces 18, 20, and 22 to eliminate the possibility of unauthorized data transmissions between user 10, network 14, and database 24. The network can be public network 14 such as the Internet or any type of private network 15. Verification server 28 is connected to database 24 via network interface 30 and networks 14 and/or 15 via interface 32. Interfaces 30 and 32 are disjunct relative to each other such that database 24 is not accessible to networks 14 or 15. Interface 32 for connecting verification server 28 to public network 14 or private network 15 could be separate interfaces as shown in Figure 1 or verification server 28 could be configured to interface both public network 14 and private network 15 using the same interface.

[0016] Figure 2 diagrams an embodiment of the present invention, generally 100, which includes router 36 connected to user machines 12, public network 14, private network 15 and high speed switch 38. Router 36 and switch 38 are for forwarding data interior to apparatus 100 as well as to and from the networks 14 and 15 connected thereto. Router 36 can be configured as a firewall for security purposes.

[0017] Figure 3 shows an embodiment of the present invention, generally 100, comprising router 46 connected to high speed switch 38 and public network 14. The Figure 3 embodiment includes router 46 configured to accept point to point tunneling type connections, on private internet provider addresses from a request router 44. Request router 44 is connected to user machines 12 and router 46 via network 14. Point to point tunneling type connections refers to a protocol that allows entities to extend their own networks through private "tunnels" over a public network such as the Internet, such that, in effect an entity can securely use a public network as its own local network. This type of interconnection is known in the art and may be referred to as a virtual private network. The Figure 3 embodiment of the present invention is configured to utilize point to point type connections such that a virtual private network is established between apparatus 100 and user machines 12. Referring again to the Figure 3 embodiment of the present invention, a third router 48 is connected to switch 38, public network 14 and private network 15 for retrieving data from networks 14 and 15.

[0018] Referring to Figure 4 a flowchart is generally indicated at 50. The flowchart 50 represents a method used according to the present invention for providing access to authenticated documents contained in computer network 14 or

15 utilizing user machines 12 and apparatus 100. The method utilized by server 16 begins at 52. A user request for content from the network is input at 54. The user request could be a programmatic request from a remote computer. Database 24 is accessed at 56 and authenticating information for the particular content requested is searched for and retrieved therefrom. At 58 a determination is made whether or not database 24 contains information regarding the particular content requested as well as the authenticity status of the content if it exists in the database 24. If the authenticity status of the requested content is negative or if the requested content is not indexed in database 24, then a refusal is returned to the user at 70. If the requested content is indexed in database 24 and the authenticity status therefor is determined positive at 58, network 14 or 15 is accessed at 60 and the requested content is copied therefrom. A checksum is calculated at 62 using the authenticating information retrieved from database 24 at 56 and a predetermined algorithm. At 64 a comparison is made between the checksum calculated at 62 and the stored checksum for the particular content retrieved from database 24 at 56, if the checksums are equal, the requested content is returned to the user at 72 and the method is terminated. Otherwise, if the checksums are not equal at 64, the authenticity status for the content requested is updated to a negative or not trusted status at 66. The content requested and determined not authentic at 64, and therefore not trusted, is forwarded to a quality assurance department at 68. A refusal is returned to user machine 12 at 70 and the method is terminated.

[0019] Referring to Figure 5 a flowchart is generally indicated at 75. The flowchart 75 represents a method used according to the present invention for calculating a checksum for a document. The method for calculating a checksum, utilized by server 16 and verification server 28 begins at 76. Counters for the number of characters in the document (start) and the checksum value (TCS sum) are initialized to zero at 78. Also, at 78 a length counter (length) is initialized to the number of characters in the document. Database 24 is accessed at 80 to determine if seed values exist for the content for which a checksum is being calculated. If seed values exist in database 24 for the particular document, LR seed value (LR) for the length right, and RL seed value for the return length are retrieved from database 24. If no seed values exist for the document, seed values are determined for length right (LR) and return length (RL) at 82 using a random number generator, and stored in database 24. A character by character traversal of the content of the document

begins at 84 with the retrieval of the first character. At 86 a determination is made to see if more characters exist or if the traversal of the content is complete. If the traversal of the content of the document is complete, the checksum, TCS sum is returned at 88 and the method for calculating a checksum for a document terminates at 88. Otherwise, if the character traversal is not complete, at 90, the ASCII value of the character is used to increase the TCS value as follows: First, the value of (LR seed * start * character) is added to the value of TCS sum where character is the ASCII value of the character; Secondly, the value of (RL seed * length * character) is added to the value of TCS sum where character is the ASCII value of the character. At 92, the start and length counters are incremented and decreased by one respectively. The next character in the document is retrieved at 94, and returned to the end of content determination step at 86. The method terminates and the TCS sum is returned, at 88, when the traversal of the characters in the document is complete.

[0020] Alternatively, a two-pass method for calculating the checksum uses predetermine seed numbers and includes the steps of a) retrieving indexed seed numbers for the document from database 24; b) traversing a forward pass of the data stream of the content of the retrieved document and calculating a first value for each position in said data stream using the seed numbers; c) traversing a reverse pass of the data stream of the content of the retrieved document and calculating a second value for each position in the data stream using the seed numbers; and d) summing the first value second values.

[0021] Referring to Figure 6 a flowchart is generally indicated at 95. Flowchart 95 represents a method used by verification server 28 according to the present invention. Verification server 28 constantly cycles through database 24 and retrieves the information stored therein for identifying and authenticating the particular documents contained in the network 14 or 15. Verification server 28 retrieves from network 14 or 15 the content of the document identified and checks the authenticity thereof using the information retrieved from database 24 and the checksum calculation shown in Figure 5 and described above. A preferred method of authentication utilized by verification server 28 is outlined in flowchart 95. The method starts at 98. Database 24 is accessed and the list of identification and authentication information for all documents indexed in database 24 is retrieved at 102. In particular, the information retrieved at 102 includes the TCS sum, authentication status, seed values, and address information for each document

indexed in the list. The first entry from the list is read at 104. A determination is made at 106, whether or not the entry read at 104 is the end of the list. If the entry is determined to be the end of the list at 106, verification server 28 returns to database 24 at 102 and retrieves the entire list stored therein. Otherwise, at 108, the content identified by the current entry is retrieved and copied from network 14 or 15. At 110. a checksum is calculated for the content retrieved using the algorithm described above and shown in Figure 5. One skilled in the art will recognize that any appropriate algorithm could be utilized and that the one identified in Figure 5 is merely a preferred algorithm identified by the Applicant. At 112 a determination is made whether or not the content retrieved is authentic by comparing the checksum calculated at 110 with the checksum value read from database 24 for the particular document. If the checksums are determined to be equivalent, the retrieved content is determined authentic, and the server 28 reads the next entry in the list and returns to 106. Otherwise, if the checksums at compared at 112 are not equal, the content is determined not authentic and the authenticity status for the entry is updated to negative or not trusted in database 24. If determined not authentic, or not trusted, the content of the document is forwarded to a quality assurance department for further review at 116. Thus, according to the present invention, verification server 28 continuously traverses database 24 checking the authenticity of each entry indexed therein.

[0022] Referring to Figure 7, tables 105 and 115 represent one embodiment of the format of database 24 for each indexed document stored therein, according to the present invention. At 122, an identification for the document is stored in the form of an integer. At 124, the checksum (TCS sum), is stored for the content of the document as an integer. The authenticity status for the content of the document is stored as a character at 126. At 128, and 130 seed values (LR) for the length right, and (RL) for the return length, respectively are stored in database 24. Identification integer 122 is also used to access the content identification represented by table 115 wherein the Universal Resource Locator (URL) addresses are stored at 136 for each document indexed in database 24 which is contained in public network 14. If the document is contained in a private network an appropriate address therefor would be stored at 136. A content identifier for each document is stored at 136 in database 24.

[0023] The applicant has suggested that some of the many uses of the trusted

content server of the present invention are applications involving internet access for schools, applications related to the financial industry as well as many other industries wherein the authenticity of the content of documents is important. One skilled in the art will recognize that there are many applications wherein the present invention can be used to authentic the content of documents stored on a network.

[0024] Thus, while the present invention has been described with preferred embodiments thereof, it will be understood that many modifications will be readily apparent to those skilled in the art. Therefore, it is intended that this invention be limited only by the following claims and the equivalents thereof.